JP9-1999-0266
US (YOR)

证　明

本证明之附件是向本局提交的下列专利申请副本

申　　日：　2000 01 07

申　　号：　00 1 00915.X

申 请 类 别：　发明专利

发明创造名称：　有效地收集、整理和访问证书吊销表的系统和方法

申 请 人：　国际商业机器公司

发明人（设计人）：刘友祥；田忠；徐景民

CERTIFIED COPY OF
PRIORITY DOCUMENT

中华人民共和国
国家知识产权局局长　姜颖

2000 年 6 月 19 日

权 利 要 求 书

1. 一种有效地收集、整理和访问证书吊销表（CRL）的系统，包括：

多个认证机构（CA），每个认证机构都以证书吊销表的形式维护和发布已被吊销的数字证书，并且各个认证机构发布证书吊销表的方式可以不同；

多个与认证机构发布证书吊销表的方式相关的 CRL 检索代理，用于收集、整理来自多个认证机构的证书吊销表；

多个 CRL 数据库，用于存储来自多个 CRL 检索代理的经其整理后的证书吊销表或其副本；以及

CRL 访问用户接口，为用户访问 CRL 数据库中的证书吊销表提供统一的应用程序接口。

2. 根据权利要求 1 的有效地收集、整理和访问证书吊销表的系统，其中多个 CRL 数据库包括中央 CRL 数据库和多个 CRL 副本数据库，中央 CRL 数据库用于存储来自多个 CRL 检索代理的经其整理后的证书吊销表，多个 CRL 副本数据库用于存储中央 CRL 数据库中证书吊销表的副本。

3. 根据权利要求 1 的有效地收集、整理和访问证书吊销表的系统，其中多个与认证机构发布证书吊销表的方式相关的 CRL 检索代理包括一个 LDAP/CRL 检索代理，用于周期性地从特定的 LDAP 服务器上检测证书吊销表和更新 CRL 数据库中的证书吊销表。

4. 根据权利要求 1 的有效地收集、整理和访问证书吊销表的系统，其中多个与认证机构发布证书吊销表的方式相关的 CRL 检索代理包括一个 HTTP/CRL 检索代理，用于周期性地从特定的 HTTP 服务器上检测证书吊销表和更新 CRL 数据库中的证书吊销表。

5. 根据权利要求 1 的有效地收集、整理和访问证书吊销表的系统，其中多个与认证机构发布证书吊销表的方式相关的 CLR 检索代理包括一个 RFC 1424/CRL 检索代理，用于周期性地发送 RFC1424CRL 检索请求和接收 CRL 检索应答。

6. 根据权利要求 1 的有效地收集、整和访问证书吊销表的系统，其中多个与认证机构发布证书吊销表的方式相关的 CRL 检索代理包括一个 Http 接收代理，该代理由 HTTP 请求触发，该代理对请求者的权限进行验证，如果验证成功，该代理则将请求者发送来的 CRL 存储在 CRL 数据库中。

7. 根据权利要求 1 的有效地收集、整理和访问证书吊销表的系统，其中多个与认证机构发布证书吊销表的方式相关的 CRL 检索代理还对检索到的证书吊销表的完整性和合法性进行检验。

8. 根据权利要求 1 的有效地收集、整理和访问证书吊销表的系统，其中，多个 CRL 数据库之间可以采用某种复制结构以保持数据库之间的致性。

9. 根据权利要求 2 的有效地收集、整理和访问证书吊销表的系统，其中，中央 CRL 数据库和多个 CRL 副本数据库之间可以采用 Hub-and-Spoke 复制结构。

10. 根据权利要求 1 的有效地收集、整理和访问证书吊销表的系统，适用于收集、整理和访问各种类型的黑名单。

11. 一种在通过数字证书实现安全通信的网络中，有效地收集、整理和访问证书吊销表（CRL）的方法，其中多个认证机构（CA）都以证书吊销表的形式在网络中维护和发布已被吊销的数字证书，并且各个认证机构发布证书吊销表的方式可以不同，所述方法的特征在于步骤:

根据认证机构发布证书吊销表的方式来建立多个 CRL 检索代理，用于收集、整理来自多个认证机构的证书吊销表;

将来自多个 CRL 检索代理的经其整理后的证书吊销表或其副本分别存储在多个 CRL 数据库中；和

通过统一的应用程序接口访问 CRL 数据库。

12. 根据权利要求 11 的有效地收集、整理和访问证书吊销表的系统，其中多个 CRL 数据库包括中央 CRL 数据库和多个 CRL 副本数据库，中央 CRL 数据库用于存储来自多个 CRL 检索代理的经其整理后的证书吊销表，多个 CRL 副本数据库用于存储中央 CRL 数据库中证书吊销表的副本。

13. 根据权利要求 11 的有效地收集、整理和访问证书吊销表的方法，适用于收集、整理和访问各种类型的黑名单。

说　　明　　书

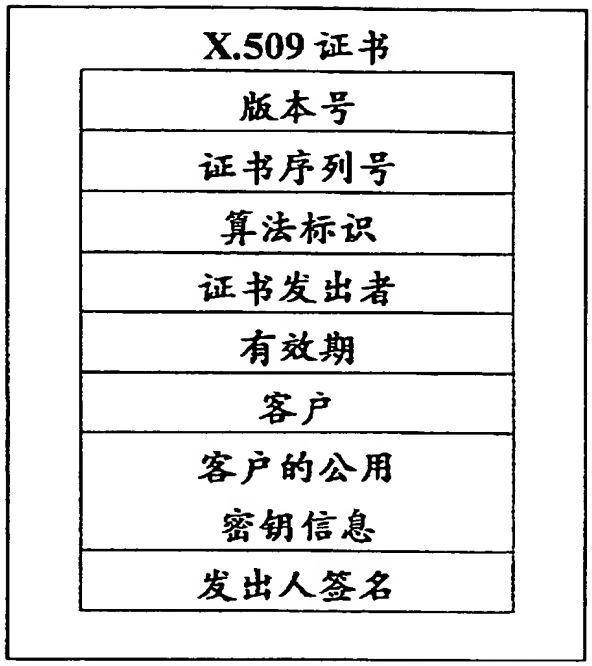
有效地收集、整理和访问证书吊销表的系统和方法

本发明涉及数字证书的管理，具体地说，涉及有效地收集、整理和访问数字证书吊销表。

实现电子商务的系统正在变得越来越广泛，这部分地由于象因特网之类全球计算机网络的出现，部分地由于公用密钥密码术的发展与成熟，它提高了这种商业活动的安全性。于是，在一些报告中已经预见了公共密钥密码术对于电子商务的应用，诸如：国际通信联盟（ITU，前身是CCITT）的建议X.509。

为了安全地进行电子商务活动，根据传统方法，每个用户有一对相关密钥，即一个私人密钥和一个公用密钥。但是，公用密钥只是一个数值，它与任何人（包括要认证其消息的人）没有任何内在关联。数字签名的广泛商业应用要求有可靠的信息把公用密钥与识别出的人们关联起来。然后，那些被识别出的人们的消息能通过使用这些密钥加以认证。

数字签名证书满足这种要求，这些证书一般由可信任的第三方发出，这些第三方被称作认证机构（CA），它们证明（1）发出的证书的认证机构已经识别出证书的主体，（2）（在证书中）指定的公用密钥对应于由证书主体掌握的私人密钥。为了保证其后能核实一证书的可信性，认证机构在发出证书时要对其进行数字签名。在前文引述的X.509标准中规定了数字签名证书的一般结构，典型的X.509证书具有以下格式：



一般在证书中要规定其有效期。过了有效期的证书为无效证书。除过期的证书外，无效证书还包括:

· 已被吊销的证书（即已被签发此证书的认证机构声明为永久无效的证书）；以及

· 已被暂停的证书（即已被签发此证书的认证机构声明为暂时无效的证书）。

吊销和/或暂停证书是最大限度地减小由于认证机构或客户造成的错误后果的重要手段。认证机构可以通过吊销证书来避免由于证书中的不准确性造成的进一步损失。客户可以通过吊销一个证书来防止信赖使用受危害的私人密钥（例如丢失的或被偷的私人密钥）产生的伪造数字签名。根据 ITU X.509，那些由于吊销而变为无效的证书一般被列入证书吊销表（CRL）。在 ITU X.509 中未考虑暂停或暂时无效，所以暂停或暂时无效的证书可以包括在 CRL 中或可能没有被包括在其中。由于时效使其变为无效的证书无需列入 CRL，因为每个证书中都包含了其有效期。一般每个认证机构都维护一个 CRL，并以特定的方式定期对 CRL 进行更新和发布。

在实践中，传统的基于 CRL 的电子商务系统按如下方式工作：在一客户能造成一个可核实的数字签名之前，该客户必须作出安排，使一个认证机构发出一个能以客户的公用密钥来标识该客户的证书。该客户收回并接受这个被发出的证书，然后造成数字签名，并把该证书的拷贝附着在每个数字签名上。当一个事务的另一方收到这种数字签名时，这另一方必须与认证机构核对，一般是通过在线数据库，以确定该证书当前是否有效。如果有效，而且该数字签名能被证书中的公用密钥核实，则另一方可以信赖这个数字签名。

现代的电子商务系统一般都建立在开放式互联网络的基础上，由于用户可能使用任何一个现有的 CA 作为其证书签发机构，所以这样的电子商务系统一般需要访问来自多个 CA 的 CRL。由于不同的 CA 可能使用不同的 CRL 发布机制，这就需要电子商务系统的开发者了解各种 CRL 发布机制，此外，一些 CA 还可能改变其 CRL 发布机制，这就进一步加重了应用程序开发者的负担。

此外，一些 CA 采纳诸如通过目录服务器的 CRL 在线发布机制。应用程序在需要时可以下载这些 CRL。但是实时访问 CRL 不但造价高并且对于大多数应用来说也是不必要的。此外，由于一个应用程序下载和分析的 CRL 不能被其它应用程序所共享，于是造成了系统资源的浪费。

为解决以上问题本发明提出一种有效地收集、整理和访问 CRL 的系统和方法。本发明的方法和系统通过对不同的 CRL 发布机制建立不同的 CRL 检索代理来收集、整理来自不同的 CA 的 CRL，并将整理后的 CRL 存储到中央数据库中，然后通过网络将中央数据库复制到其它机器上去。应用程序可以通过一组统一的应用程序接口来访问最近的 CRL 数据库以确定数字证书是否已被吊销，这样应用程序就不用关心各种 CRL 发布机制的细节。此外，由于 CRL 数据库中的内容可被所有应用程序所共享，所以提高了系统资源的利用率。

根据本发明的一个方面，提供了一种有效地收集、整理和访问证书吊销表的系统，包括：

多个认证机构（CA），每个认证机构都以证书吊销表的形式维护和

发布已被吊销的数字证书，并且各个认证机构发布证书吊销表的方式可以不同；

多个与认证机构发布证书吊销表的方式相关的 CRL 检索代理，用于收集、整理来自多个认证机构的证书吊销表；

多个 CRL 数据库，用于存储来自多个 CRL 检索代理的经其整理后的证书吊销表或其副本；以及

CRL 访问用户接口，为用户访问 CRL 数据库中的证书吊销表提供统一的应用程序接口。

根据本发明另一方面，提供了一种在通过数字证书实现安全通信的网络中，有效地收集、整理和访问证书吊销表的方法，其中多个认证机构都以证书吊销表的形式在网络中维护和发布已被吊销的数字证书，并且各个认证机构发布证书吊销表的方式可以不同，该方法包括步骤：

根据认证机构发布的证书吊销表的方式来建立多个 CRL 检索代理，用于收集、整理来自多个认证机构的证书吊销表；

将来自多个 CRL 检索代理的经其整理后的证书吊销表或其副本分别存储在多个 CRL 数据库中；和

通过统一的应用程序接口访问 CRL 数据库。

通过以下结合附图对本发明优选实施例的介绍，可以使本发明的目的、优点和特征更加清楚。

图 1 为根据本发明一个优选实施例的有效地收集、整理和访问 CRL 的系统的方框图；

图 2 为根据本发明优选实施例的 LDAP/CRL 检索代理的工作示意图；

图 3 为根据本发明优选实施例的 HTTP/CRL 检索代理的工作示意图；

图 4 为根据本发明优选实施例的 RFC1424/CRL 检索代理的工作示意图；

图 5 为根据本发明优选实施例的 Http 接收代理的工作示意图；

图 6 为根据本发明优选实施例的 CRL 数据库的复制结构的示意图；

图 7 为根据本发明另一个优选实施例的有效地收集、整理和访问

CRL 的系统的方框图；和

图 8 为根据本发明优选实施例的有效地收集、整理和访问 CRL 的方法的流程图。

在结合具体实施例说明本发明的方法和系统之前，首先讨论一下有关证书吊销表的一般问题，如证书吊销表的格式、证书吊销表的发布方式。

在前文中已介绍过数字证书是用来证明一个特定的公用密钥属于一个特定实体的数字文件，数字证书

· 由可信任的第三方或称作认证机构数字签署；

· 只在指定的期限内有效；

· 可被任何有权访问 CA 的公用密钥的人来验证；

· 具有一个在 CA 内的唯一的序列号。

然而，数字证书在其有效期届满之前，由于各种原因可能已被吊销，于是，每个 CA 有责任维护一个证书吊销表，并且应该不断地更新它，并使它能够被公众所得。证书吊销表中的已被吊销的证书可由其序列号来标识。

用 ASN.1（抽象语法记法.1）SEQUENCE 结构描述的 X.509 CRL 如下：

```
CertificateList  ::=SEQUENCE{
   tbsCertList          TBSCertList,
   signatureAlgorithm       AlgorithmIdentifier,
   signature                BIT STRING
}
```

其中 SignatureAlgorithm 用于标识 CA 在对 TSSCertList 结构进行数字签名时所使用的算法，其中 TBS CertList 本身用 ASN.1 SEQUENCE 结构表示如下：

```
TBSCertList  ::=SEQUENCE{
   version                 Version OPTIONAL,
   signature               AlgorithmIdentifier,
   issuer                  Name,
   thisUpdate              Time,
   nextUpdate              Time OPTIONANL,
   revokedCertificates          SEQUENCE OF SEQUENCE{
         userCertificate                CertificateSeriaNumber,
```

```
        revocationDate              Date,
        crlEntryExtension Extensions OPTIONAL
    }OPTIONAL
    crlExtensions[0]    EXPLICIT   Extensions   OPTIONAL
}
```

TBSCertList 指出 CRL 的发布者名称、发布日期、下次发布 CRL 的日期以及已被吊销的数字证书（由序列号来标识的）的清单（后两项为任选项）。

在此需要注意两点。首先，已被吊销的数字证书的清单是任选的，因为有可能某一个 CA 在应该发布 CRL 时还没有吊销任何证书。其次，尽管 CA 可能在其 CRL 中指定了下次预订的发布 CRL 的日期，但这并不防碍 CA 在紧急情况下以更快的频率发布 CRL.

对于 CA 来说，通常有两种发布 CRL 的方式，即“pull（拉）”和“push（推）”。在“pull”方式下，验证者（需要验证某个数字证书的状态的用户）可以在需要时从 CA 下载 CRL. 而在“push”方式下，CA 定期地向注册的验证者发送 CRL。

由 X.509 定义的认证框架最初设计成工作在 X.500 目录环境下。X.500 规定使用与 CA 实体相关的目录属性来存储 CRL. X.500 还定义了客户用来访问目录的 DAP（目录访问协议）。然而，由于 DAP 协议太复杂，使其难于在诸如 PC 等机器上运行。于是设计了 LDAP（轻型目录访问协议），减少了目录客户机上 X.500 访问的负担，使这种目录可应用于各种机器和应用程序。LDAP 可以直接运行在支持 TCP/IP 的机器上。验证者可以使用“pull”方式从 LDAP 服务器中检索 CRL。

然而，近期 X.500 目录服务不会在因特网上迅速普及起来，人们还可能开发其它的使用现有因特网基础设施的CRL发布和访问方法。在Privacy-Enhanced Mail（保密增强型信箱）中定义了一个这样的方法。根据 PEM，IPRA（Internet Policy Registration Authority）应当和 PCA （Policy Certification Authorities）进行协调以提供一个安全可靠的包括 IPRA、PCA 以及所有其它 CA 发布的 CRL 的数据库. 通过由每个 PCA 维护的信箱来提供对数据库的访问。验证者可以使用 RFC1424 中定义的机制检索来自具体一个或多个电子邮件地址的 CRL。CRL 检索方法根据相关的 PCA 是否支持非请求型 CRL 发布方式而或者工作于“pull”方式或者工

作于“push”方式.

以上已讨论了证书吊销表的格式和证书吊销表的发布方式，下面就结合具体实施例描述一下根据本发明的用于收集、整理和访问证书吊销表的方法和系统。

在本发明的用于收集、整理和访问证书吊销表的系统中，使用中央数据库来存储由各个 CA 吊销的所有数字证书。对于各种不同的 CRL 发布方式，建立不同的 CRL 检索代理，这些代理周期性地检索来自不同 CA 的 CRL，并对 CRL 进行整理，之后存入中央 CRL 数据库。为了便于用户访问 CRL，建立多个中央 CRL 数据库的副本数据库，并提供统一的应用程序接口。

图 1 示出根据本发明一个优选实施例的用于访问 CRL 的系统的方框图。图 1 所示的系统是基于 Lotus Domino 的。 Domino 群件是 Lotus 公司于 1996 年 11 月宣布的群件产品，即 Notes 4.5 的服务器版本。在这个群件中，集成了函件处理、群件应用和因特网出版功能。它采用独创的页式数据库系统（page database system）大大降低了连接管理的复杂性，管理人员可以高效地管理来自不同用户和部门的内容，是一个性能价格比较高的 Internet/Intranet 管理平台。利用它的内置开发工具，用户可以迅速开发安全的交互式应用程序，并且很容易与企业已有的数据系统集成。在图 1 所示的系统中目前支持三种 CRL 检索代理，当然，正如本领域一般技术人员所理解的那样，在此基础上可以很容易地集成其它 CRL 检索代理。从检索到的 CRL 提取被吊销的证书并将其存储在称为中央 CRL 数据库的 Domino 数据库，中央 CRL 数据库被复制到其它的 CRL 副本数据库中，这些数据库在其它相连的 Domino 服务器上。还提供一组基于 Java 的 CRL 访问 API，用于电子商务系统以充分利用就近的 Domino 服务器上的经整理后的 CRL，而不用关心各个 CA 是如何发布 CRL 的。

尽管对不同的 CA 可能使用不同的 CRL 检索方法，但所有的方法都必须包括一个从指定的地址下载 CRL 的过程，对下载的 CRL 进行验证以保证该 CRL 确实是由特定 CA 发布的，并把下载的 CRL 保存在中央 CRL 数据库中。作为一个例子，一个特定 CA 将其 CRL 放入 LDAP

目录，驻留在中央 CRL 数据库中的 Domino 代理周期性地运行以通过 LDAP 协议检索来自指定 LDAP 服务器的 CRL 并相应地更新中央数据库。中央数据库中的任何变化将被复制到其它 CRL 副本数据库中。这不仅使 CRL 数据库管理更容易，而且还使一个电子商务系统能够更容易、迅速、低成本地访问 CRL 数据库. 当一个电子商务系统想确定一个证书是否已被吊销时，它们只需调用 API 来对最接近的 CRL 副本数据库进行访问。用于 CRL 访问的 API 然后调用 NOI（Notes Object Interface）访问 Domino CRL 数据库，判断证书是否被列在 CRL 中，并将结果返回给电子商务系统。

以下结合附图详细介绍图 1 所示系统的各个组成部分.

1. 中央 CRL 数据库

· 用于 CRL 数据库的 Domino 表单（form）

CRL 数据库包括从三个表单中产生的文档，这三个表单即：Trusted Certificate Authority（认证机构）表单、Revoked Certificate（吊销的证书）表单和 Memo 表单。Trusted Certificate Authority 表单主要包括以下字段.

字段名称	存储的数据
Distinguished Name	符合 RFC 1779 的 CA 名称
Certificate	CA 的 X.509 证书
This Update	CA 上次更新 CRL 的时间
Next Update	CA 下次更新 CRL 的时间
CRL Number	CA 的当前 CRL 序号
LDAPURL	符合 RFC 2255 的 LDAP URL
HTTPURL	HTTP URL
PCAMailbox	用于 RFC 1424 CRL 服务的 PCA 电子邮件地址

Distinguished Name 字段代表符合 RFC 1779 的可以与其它 CA 名称相区别开来的 CA 名称，Certificate 字段以 Base 64 编码的 DER 格式保持 CA 的 X.509 V3 证书.

Certificate 字段用于验证由该 CA 签发的证书和 CRL。为了避免输入错误，可以用 Clipboard 或本地的证书文件作为该字段的输入源。This Update、Next Update 和 CRL Number 字段从最近检索到 CRL 中获得

值。Next Update 和 CRL Number 字段可以为空。CRL Number 字段用于存放 CA 的当前 CRL 序号。该字段使用户可以判断一个特定的 CRL 是否替换其它 CRL。LDAPURL 字段包含符合 RFC 2255 的 LDAPURL，LDAP 检索代理使用该字段检索来自特定 LDAP 服务器的 CRL。HTTP 检索代理使用 HTTPURL 字段检索来自特定 HTTP 服务器的 CRL。PCAMail box 字段包括用于 RFC1424 CRL 服务的 CA 的 PCA 电子邮件地址。如果 PCA 支持非请求型 CRL 发布方式，则该字段可能为空。

将从检索到的 CRL 中提取的每个被吊销的证书存储在一个由 Revoked Certificate 表单创建的文档中，Revoked Certificate 表单包括以下字段:

字段	存储的数据
Distinguished Name	满足 RFC 1779 的 CA 名称
Serial Number	被吊销的证书的顺序号
Revoke Date	证书被吊销的日期
Revocation Reason	证书被吊销的原因

在 Revoked Certificate 表单中，除了 Revocation Reason 字段以外，所有字段都是强制型的。Distinguished Name 字段和 Serial Number 字段唯一地标识一个被吊销的证书。Revocation Reason 字段用于标识吊销证书被吊销的原因。

Memo 表单用于 RFC 1424 PEM 消息，该表单主要包括以下字段。

字段	存储的数据
From	PEM 消息发送者的电子信箱地址
To	PEM 消息接收者的电子信箱地址
Date	PEM 消息的发送日期
Subject	PEM 消息的主题
Body	PEM 消息的主体

· 用于 CRL 数据库的 Domino 视图

在该 Domino 数据库中建立三个视图：Trusted Certificate Authorities 视图；Revoked Certificates\ By Issuer 视图和 Revoked Certificates\ By Serial Number 视图，用于加速对特定 CA 和/或吊销的证书的检索。

Trusted Certificates Authorities 视图具有以下各列：Distinguished

Name、Current CRL Update Time、Next CRL Update Time 和 Current CRL Number 列，这些列的值来自于每个 Trusted Certificate Authority 文档的相应字段。在该视图中，“Distinguished Name 是用于自动排序列。

Revoked Certificates\ By Issuer 视图具有以下各列“Distinguished Name、Serial Number、Revoked Date 和 Revocation Reason 列，这些字段的值来自于每个 Revoked Certificate 文档的相应字段。在该视图中，“Distinguished Name”是主排序列，“Serial Number”是次排序列。此外，“Distinguished Name”还是分类列。

Revoked Certificates\ By Serial Number 视图和 Revoked Certificate\ By Issuer 视图所包含的列相同，但顺序不同，该视图所包含的列的顺序为：“Serial Number、Distinguished Name、Revoked Date 和 Revocation Reason”。在该视图中，“Serial Number”是主排序列，“Distinguished Name”为次排序列。

· Domino 代理(agent)

CRL 数据库还具有以下 Java Domino 代理：LDAP Retriever（检索）、HTTP Retriever（检索）、RFC 1424 Requester（请求）、RFC 1424 Receiver（接收）和 Http Receiver（接收）。LDAP Retriever 代理、HTTP Retriever 代理和 RFC 1424 Requester 代理是后台代理，LDAP Retriever 代理周期性地从 LDAP 服务器或 X.500－LDAP 网关检索来自 CA 的 CRL，并将 CRL 存储在 CRL 数据库，而 HTTP Retriever 代理周期性地从 HTTP 服务器上检索来自 CA 的 CRL。此外，RFC 1424 Requester 代理每隔一定时间间隔就向 PCA 信箱发送 RFC 1424 CRL 检索请求消息。仅当有新的信件到达时，RFC 1424 Receiver 代理才被激活，然后该代理从到达的信件中检索 CRL，将检索到的 CRL 存储在 CRL 数据库中。Http Receiver 代理由 HTTP 请求触发。它对请求者的权限进行验证。如果验证成功，该代理将发送来的 CRL 存储在 CRL 数据库中，所以 HTTP 任务必须运行在宿主 Domino 服务器上。该代理提供了一种便于加入其它外部 CRL 检索方法的工作方式，它只需按如下所示在 HTTP POST 消息中发送已收到的 CRL：

```
POST/ X509CRL. nsf/ HttpReceiver? OpenAgent HTTP/ 1.0
Conternt-length: <content length>
Content-type: application/ pkix-crl
Content-transfer-encoding: base 64

<base 64 encoded CRL>
```

然而，LDAP Retriever 代理是一个非限制性代理，因为该代理将进行网络 I/O 操作，所以为了使该代理运行在服务器上，必须修改公用名称和地址薄中的服务器记录。

2. LDAP 检索代理。

如图 2 所示，LDAP 检索代理与 LDAP 服务器相连，以检索 CRL 并更新 CRL 数据库。

当前有两个用于 LDAP 的 Java 接口：JDAP 和 JNDI。JDAP 是以 IETF 草稿定义的 LDAP 类库。在用于 Java 的 Netscape Directory SDK 中支持 JDAP。JNDI（Java Naming and Directory Interface，Java 命名和目录接口）是 Java Enterprise API 集的一部分，许多销售商，包括 IBM、HP、Novell 等都支持它。

LDAP 服务器在进行其它操作之前，可能需要绑定操作以对客户机的身份进行认证。在正常情况下，CA 的 CRL 属性是公众可获得的，于是匿名绑定操作就足够了。LDAP V2 客户机必须以连接的第一个协议数据单元（PDU）发送绑定请求，而 LDAP V3 客户机不需要进行绑定操作，由于 LDAP V3 服务器自动将不带现有绑定的操作看作是匿名操作。为了与 LDAP V2 服务器兼容，在进行其它 LDAP 操作之前我们总是请求匿名绑定操作。

在绑定操作之后，LDAP 检索代理使用特定的 LDAP URL 从 LDAP 服务器中获得 CA 最近的 CRL。然后，该代理使用检索到的 CRL 更新 CRL 数据库。

3. HTTP 检索代理

HTTP 检索代理的工作情况与 LDAP 检索代理相类似，如图 3 所示。HTTP 检索代理周期性地从 HTTP 服务器上检索来自 CA 的 CRLs。

4. RFC 1424 检索代理。

在前述中我们提到通过由每个 CA 的 PCA 维护的信箱可以提供 RFC 1424 CRL 检索服务。如果想得到 CA 最新的 CRL，你必须用 PCA 注册

或向PCA信箱发送一个CRL检索请求.PCA将发回一个包含请求的CRL的 CRL 检索应答消息。CRL－检索请求消息和 CRL－检索应答消息都是 PEM（保密加强型消息）。所以必须使用信箱和 PEM 用户代理来发送 CRL－检索请求消息和接收 CRL－检索应答消息。

在公用名称和地址簿中的 Domino Mail-In 数据库记录提供了一种直接将电子邮件接收到 Notes 应用中的措施，一般将这种应用程序称为信件使能应用，中央 CRL 数据库就是这样一种信件使能应用。如在前述讨论的，在 CRL 数据库中驻留有两个代理：RFC 1424 Recevier 和 RFC 1424 Requester，用于完成访问 RFC 1424 CRL 服务的任务。图 4 描述这种情况。

如果 PCA 支持非请求型 CRL 发布，即当最新 CRL 可得时，PCA 自动向用户信箱发送 CRL－检索应答消息，则可以取消对 RFC 1424 Requester 代理的调度。

RFC 1424 Requester 代理监听到来的 CRL 检索应答消息，验证检索到的 CRL 并将它们存储在 CRL 数据库中。

由于 PCA 通常使用标准的因特网邮件地址，所以用于 CRL 数据库的宿主 Domino 服务器必须能够和因特网电子邮件服务器交换电子邮件消息。

5. Http 接收代理

如图 5 所示，Http 接收代理由 HTTP 请求触发。它对请求者权限进行验证。如果验证成功，该代理将发送来的 CRL 存储在 CRL 数据库中。

6. CRL 副本数据库

为了把 CRL 数据库分布到整个 Notes 网上，我们利用了 Notes 数据库复制功能将 CRL 数据库复制到其它 Domino 服务器上，于是电子商务系统能够容易、快速、低成本地访问最近的 CRL 副本数据库以得到最新的 CRL。

如图 6 所示，在复制过程中我们采用 Hub-and-Spoke（中心－辐射）复制结构以完成复制任务。

Hub 服务器（中心服务器）负责：

· 从所有的 CA 检索最新的 CRL

· 更新中央 CRL 数据库

· 将更新内容传播到各 spoke 服务器（辐射点服务器）。

尽管可以使用 Pull-Push（拉－推）、Pull-Pull（拉－拉）、Push-Only（只推）和 Pull-Only（只拉）等复制类型，但是本领域一般技术人员会清楚在以上情形中最适合使用 Push-Only（只推）或 Pull-Only（只拉），因为不需要从幅射点服务器向中心服务器传播任何修改。指定使用 Push-Only（只推）或 Pull-Only（只拉）只影响哪个服务器启动复制工作，或者中央报务器“推”或者辐射点服务器“拉”。只需相应地修改复制连接记录和数据库 ACL。

对于每个辐射点服务器，必须在公用名称和地址簿中创建复制连接记录。在所有这些记录中，如果在“Routing and Replication（路由和复制）”节中“Replication Type（复制类型）”字段被设置为“Push-Only（只推），则在“Basics（基本）”节的“Source Server（源服务器）”字段和“Destination server（目标服务器）”字段应该分别被指定为中央服务器和辐射点服务器。如果“Replication Type”字段被设置为“Pull-Only（只拉）”，则源服务器应该是辐射点服务器，而目标服务器应该是中央服务器。

对于“Push-Only”模式，辐射点服务器中的 CRL 数据库必须至少为中央服务器分配“Designer（设计者）”权限。然而，对于“Pull-Only”模式，中央服务器中的 CRL 数据库只需为辐射点服务器分配“Reader（读者）”权限。所以建议采纳“Pull-Only”复制模式。

5. 用于对 CRL 进行访问的 Java API

我们的系统不只检索和整理来自多个 CA 的 CRL，还为电子商务系统提供一组用于对 CRL 进行访问的 Java API。API 表示为 Java 类 CRL Access Agent。CRL Access Agent 类的构造器取 CRL 数据库的名称作为参数：

```
public CRL Access Agent (string db Name);
```

在示例 CRL Access Agent 对象之后，我们调用该类的方法获取有关特定 CA 的当前 CRL 的信息，并检验证书是否已被吊销。例如：

```
CRLAccessAgent CrlChecker;
crlChecker=new CRLAccessAgent(" RevokedCert. nsf");
if( ! crlChecker. is Revoked (aDigitalCertificate)){
   System. out. println ("The certificate is revoded!");
   return;
}
```

因为 CRL Access Agent 类使用用于 Notes Object Interface (NOI)的 Java 类来访问吊销证书数据库，则必须将 notes. jar 文件加到类路径上。

图 7 示出了根据本发明又一个实施例的有效地收集、整理和访问 CRL 的系统的方框图。如图所示，所有的 CRL 数据库不分主次，都可以接收来自 CRL 检索代理的经其整理后的证书吊销表，同时为了保持数据库之间的一致性，每一数据库都可以向其它数据库复制 CRL 更新结果。正如本领域一般技术人员所清楚的那样，在不违背本发明的精神的前提条件下，可以对以上实施例做出各种修改。

以上结合具体实施例描述了本发明的用于有效地整理和访问证书吊销表的系统。从以上有关本发明的介绍可以得出这样一种在通过数字证书实现安全通信的网络中，有效地整理和访问证书吊销表（CRL）的方法，如图 8 所示，在步骤 801，根据认证机构发布证书吊销表的方式来建立多个 CRL 检索代理，用于整理来自多个认证机构的证书吊销表。在步骤 802，将来自多个 CRL 检索代理的经其整理后的证书吊销表存储在中央 CRL 数据库中。在步骤 803，从中央 CRL 数据库向多个 CRL 副本数据库复制证书吊销表。在步骤 804，通过统一的应用程序接口访问中央 CRL 数据库或 CRL－副本数据库。

以上我们描述的 CRL 访问机制，是一种独立于具体 CA 的 CRL 发布方式的有效地整理和访问 CRL 的机制。尽管在本发明实施例中利用了 Lotus Domino 的某些先进特点，但本领域一般技术人员应清楚，这并不构成对本发明的限制。此外，本领域一般技术人员还应清楚，在稍加修改后，本发明的用于收集、整理和访问证书吊销表的系统和方法还适合用于收集、整理和访问各种类型的黑名单，所以本发明旨在包括所有的这些修改和变型，本发明的保护范围应由所附权利要求书来限定。

说 明 书 附 图

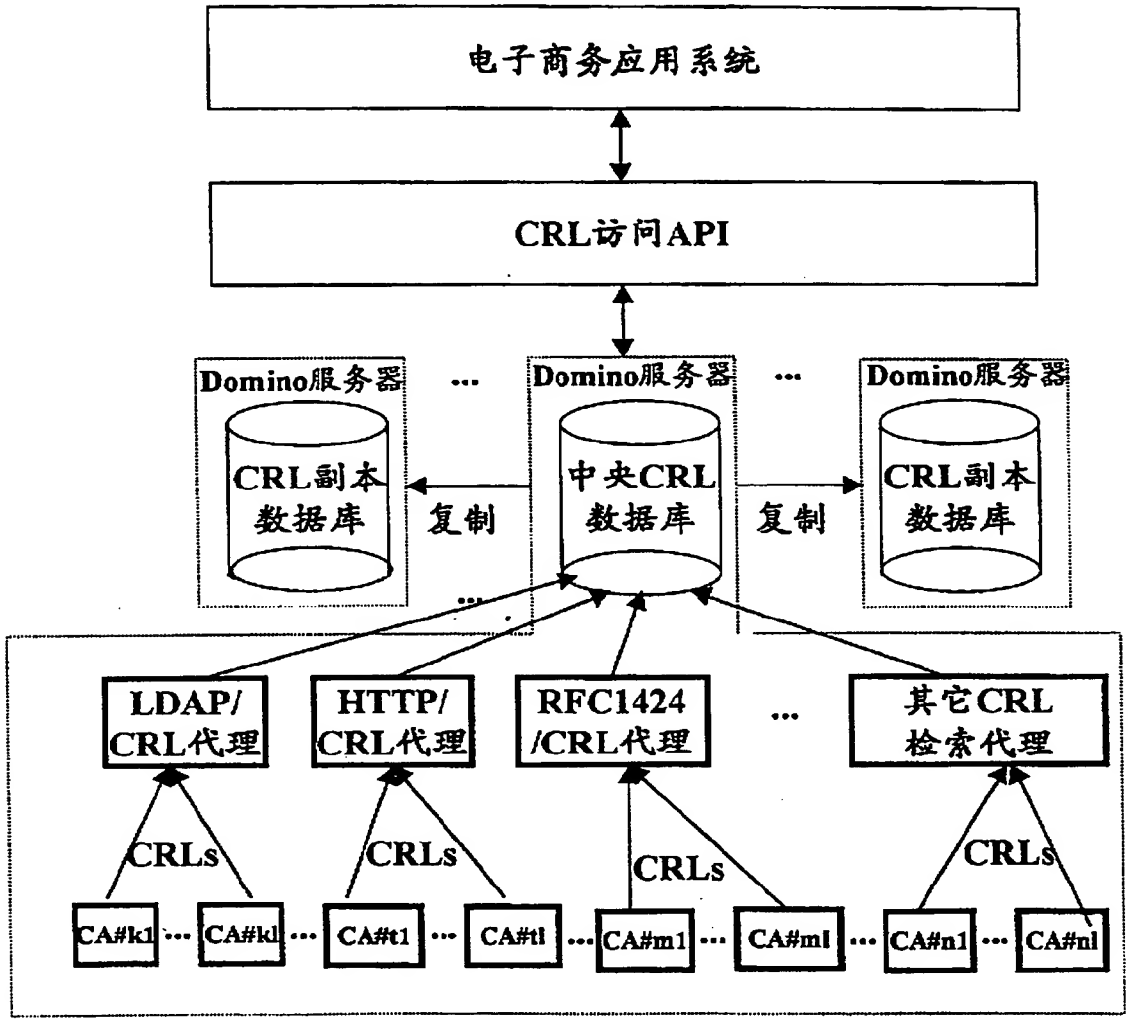

电子商务应用系统
CRL访问API
Domino服务器
Domino服务器
Domino服务器
CRL副本数据库
复制
中央CRL数据库
复制
CRL副本数据库
LDAP/CRL代理
HTTP/CRL代理
RFC1424/CRL代理
其它CRL检索代理
CRLs
CRLs
CRLs
CRLs
CA#k1
CA#kl
CA#t1
CA#tl
CA#m1
CA#ml
CA#n1
CA#nl

图1

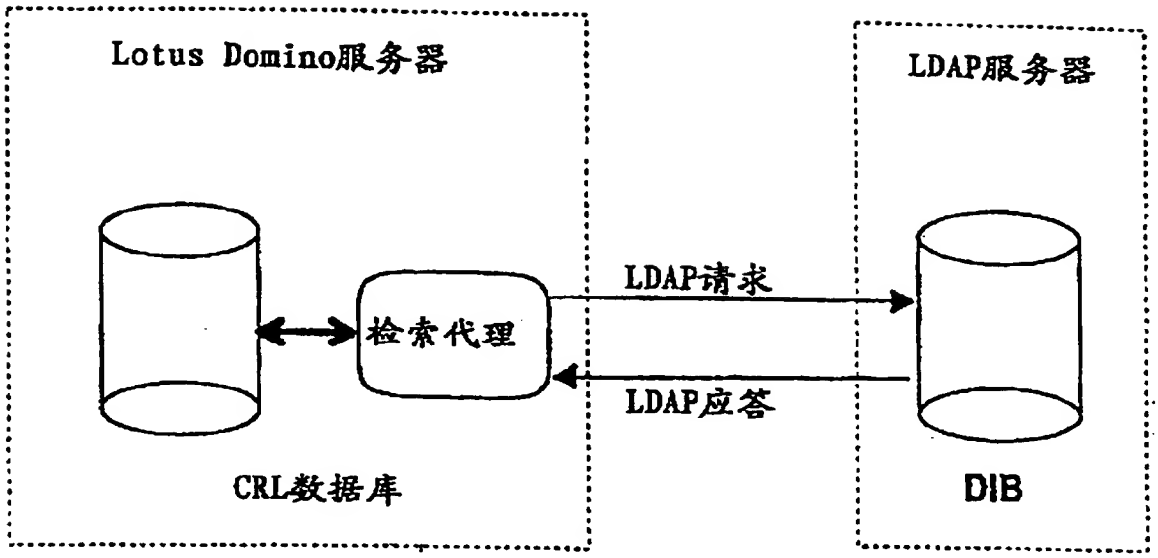

Lotus Domino服务器
LDAP服务器
检索代理
LDAP请求
LDAP应答
CRL数据库
DIB

图2

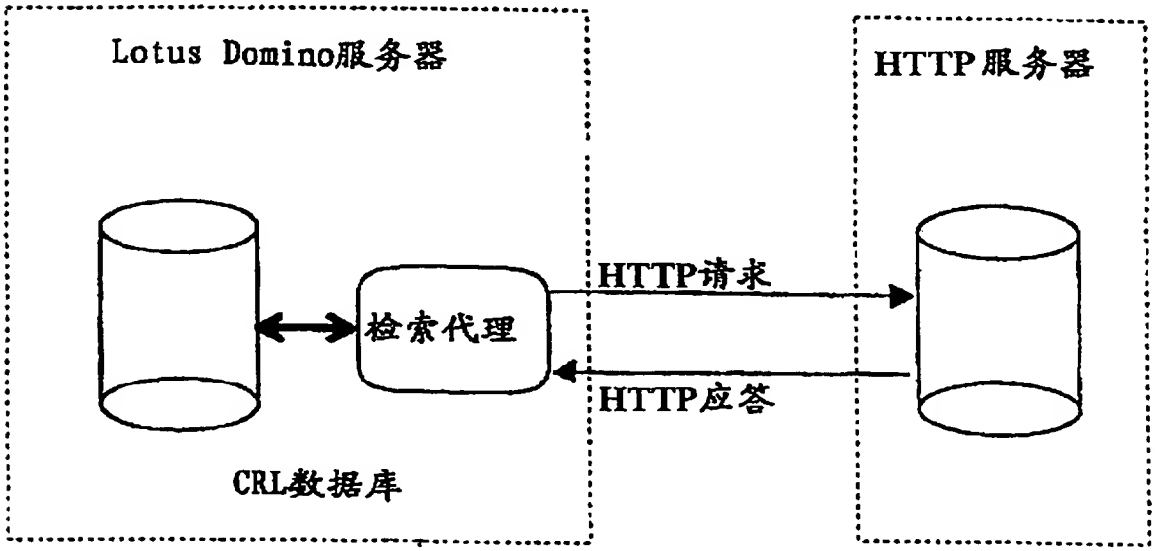
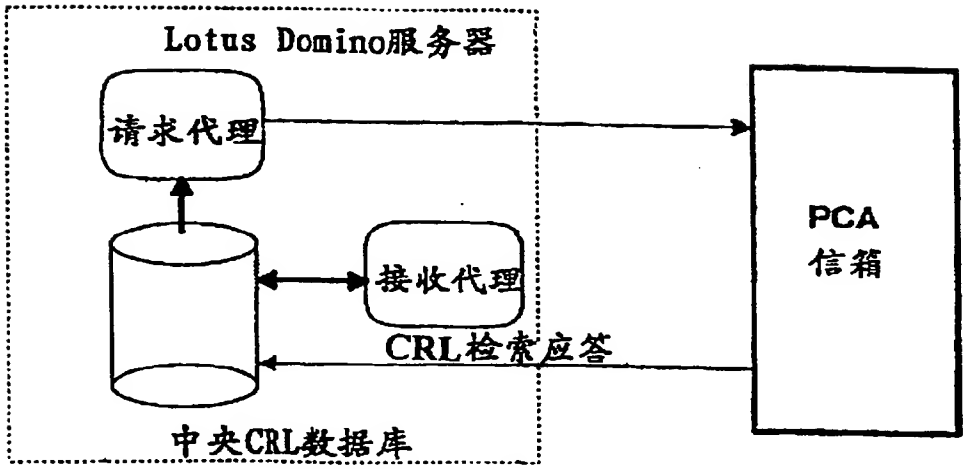

Lotus Domino服务器
HTTP服务器
检索代理
HTTP请求
HTTP应答
CRL数据库

图3

图4


Lotus Domino服务器
请求代理
接收代理
CRL检索应答
中央CRL数据库
PCA
信箱

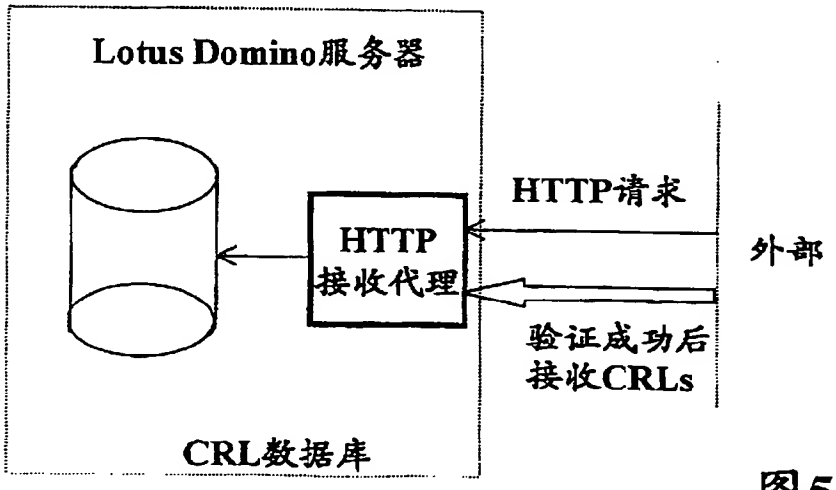

Lotus Domino服务器
HTTP请求
HTTP
接收代理
外部
验证成功后
接收CRLs
CRL数据库

图5

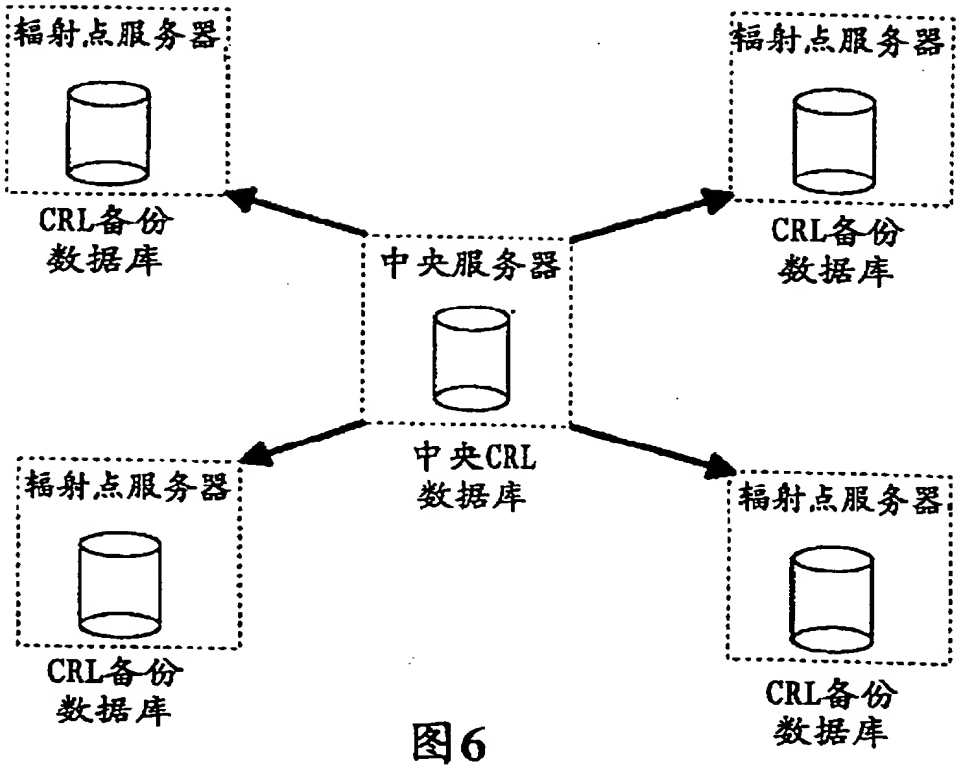

辐射点服务器
CRL备份
数据库
辐射点服务器
CRL备份
数据库
中央服务器
中央CRL
数据库
辐射点服务器
CRL备份
数据库
辐射点服务器
CRL备份
数据库

图6

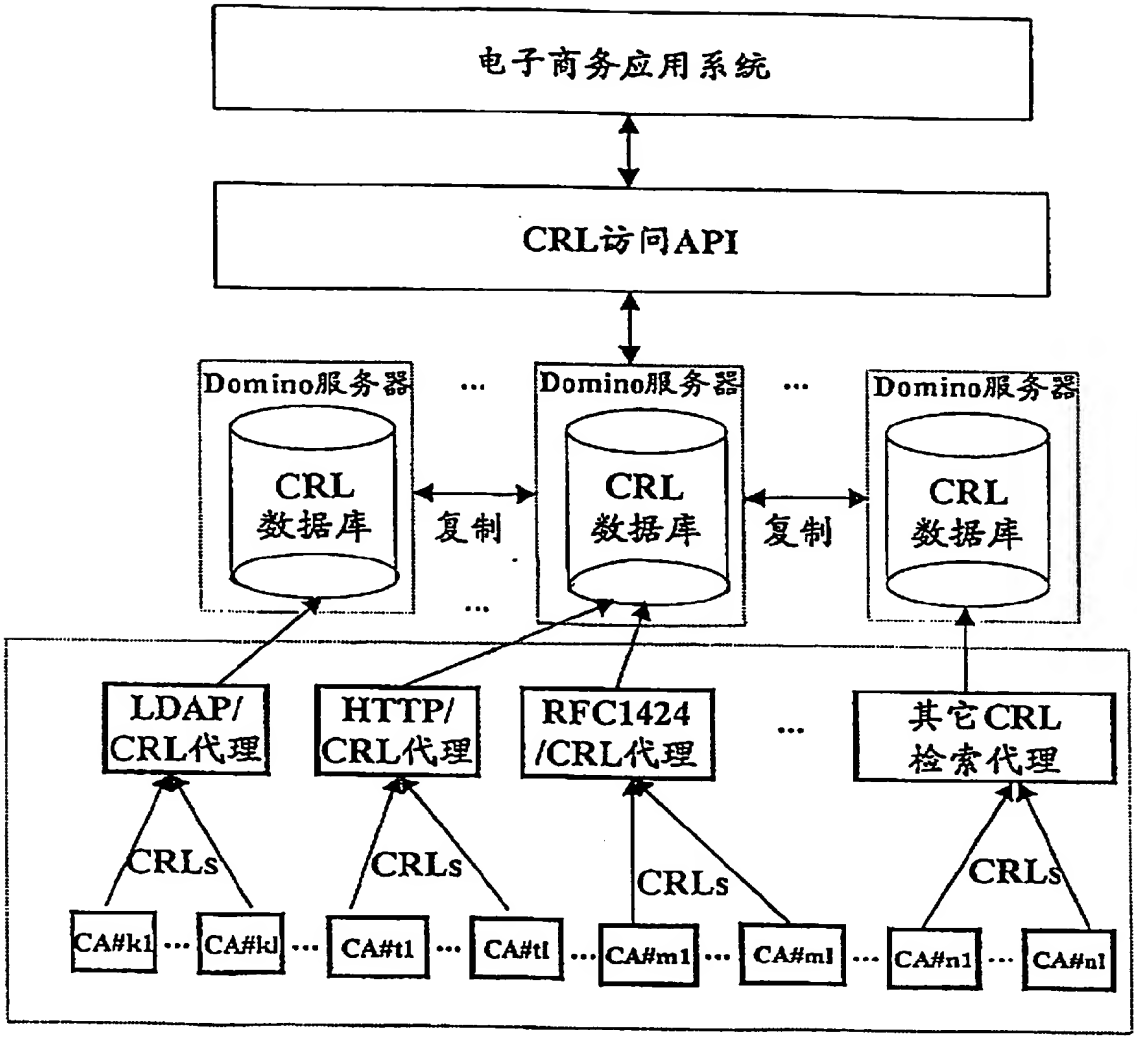

电子商务应用系统
CRL访问API
Domino服务器
CRL
数据库
复制
Domino服务器
CRL
数据库
复制
Domino服务器
CRL
数据库
LDAP/
CRL代理
HTTP/
CRL代理
RFC1424
/CRL代理
其它CRL
检索代理
CRLs
CRLs
CRLs
CRLs
CA#k1
CA#kJ
CA#t1
CA#tl
CA#m1
CA#ml
CA#n1
CA#nl

图7

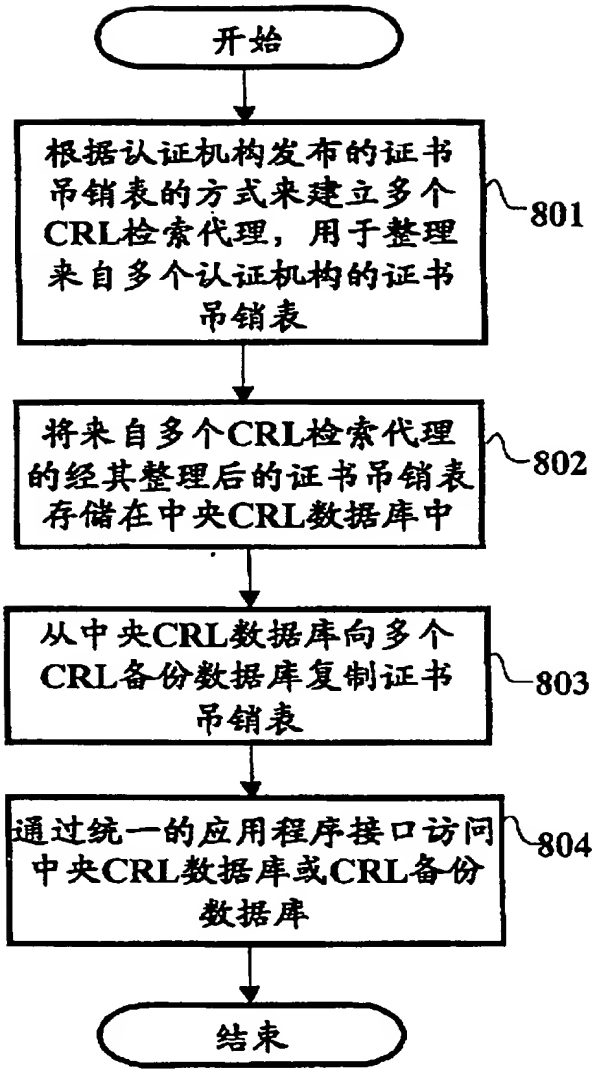

开始
根据认证机构发布的证书吊销表的方式来建立多个CRL检索代理，用于整理来自多个认证机构的证书吊销表
801
将来自多个CRL检索代理的经其整理后的证书吊销表存储在中央CRL数据库中
802
从中央CRL数据库向多个CRL备份数据库复制证书吊销表
803
通过统一的应用程序接口访问中央CRL数据库或CRL备份数据库
804
结束

图8